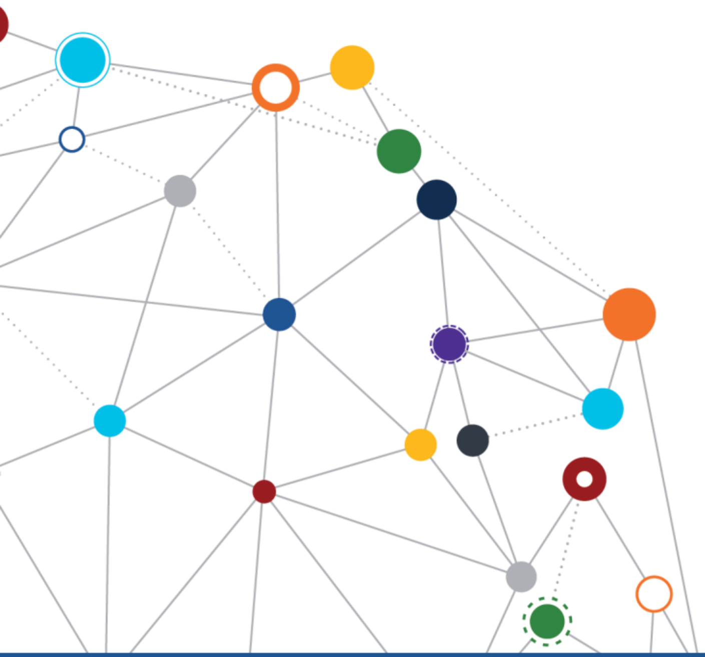
OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Authenticators and Multifactor Authentication (MFA)

March 2019 | Enterprise Program Management Office



VA
U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	3/4/2019	IAM Segment: Authenticator and Multi-Factor Authentication (MFA) approved

1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11,[1] the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) Guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) initiative.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

Single factor (SF) authentication has become a high risk for users. There is an increase in the number of data breaches that expose single pieces of evidence, or factors, such as usernames, passwords, and other sensitive information. Combined with phishing, keylogging, and other attack trends, SF authentication creates high levels of user compromise. In addition, “two step verification” methods, such as SMS (short message service) codes, have been compromised from SIM (subscriber identity module) swapping and unauthorized mobile phone number porting. SMS also presents other vulnerabilities; it is not encrypted on the provider’s network, and it is susceptible to interception.[2]

Challenges to SF authentication and some two factor authentication methods has led to increased adoption of multifactor authentication (MFA) solutions. MFA refers to the use of two or more factors to authenticate a user. Federal agencies are already adopting MFA at high rates of compliance, having implemented Homeland Security Presidential Directive 12 (HSPD-12); with the exception of mobile device conformity, which still lags behind the rest of the enterprise. External users, however, are still at risk. This is due to lack of adoption and interoperability challenges.

VA requires enterprise guidance on the design of MFA to provide consistent security and limit risk. The progression of how IAM services are engaged by users and system owners is shown in Figure 1. This Enterprise Design Pattern (EDP) document focuses on the area that is highlighted in red.

[1] Note that M 11-11 is a pending rescission. A draft OMB policy that is aligned with NIST 800-63 can be found at https://policy.cio.gov/identity-draft/.

[2] For more information on SMS vulnerabilities, refer to https://secure-voice.com/ss7_attacks/.

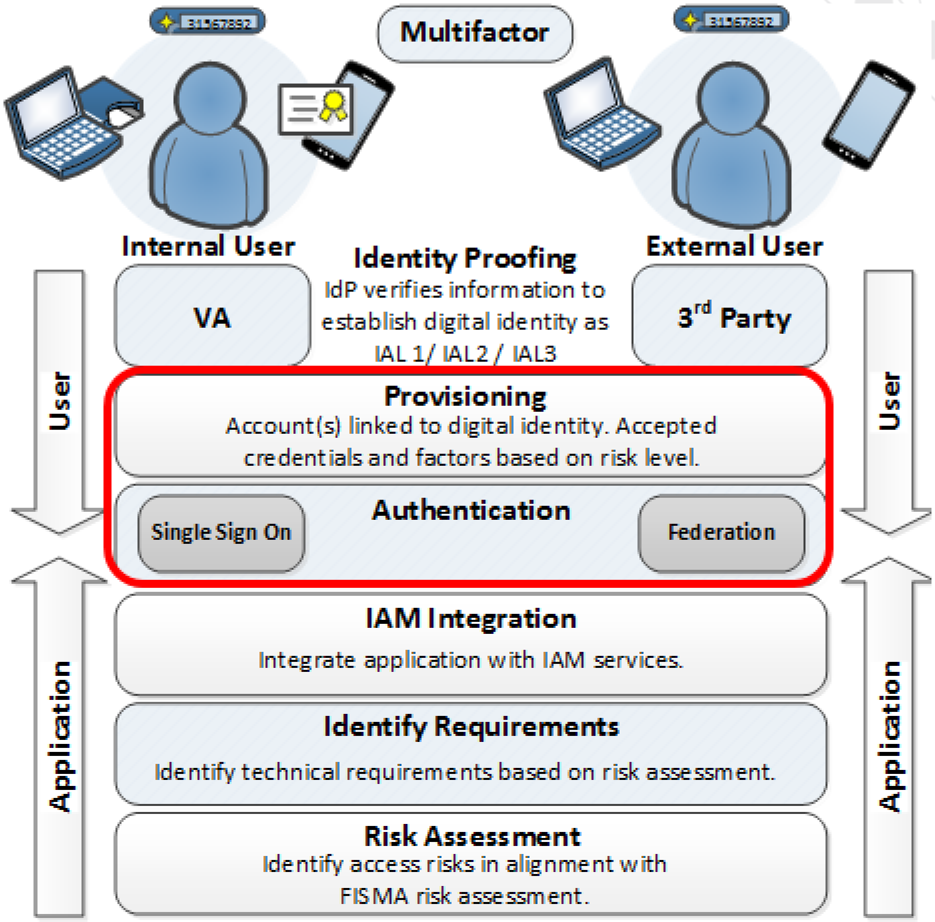

Multifactor
Internal User
External User
Identity Proofing
IdP verifies information to establish digital identity as IAL 1/ IAL2 / IAL3
VA
3rd Party
User
User
Provisioning
Account(s) linked to digital identity. Accepted credentials and factors based on risk level.
Authentication
Single Sign On
Federation
IAM Integration
Integrate application with IAM services.
Identify Requirements
Identify technical requirements based on risk assessment.
Risk Assessment
Identify access risks in alignment with FISMA risk assessment.
Application
Application

Figure 1: Overview of IAM Progression

3 Guidance

MFA authentication is not a stand-alone resolution to authentication challenges. An authenticator only confirms that the authenticating user is in possession of the hardware device, or the secret being used. To reduce the risk of unauthorized access, the authenticator must be connected to a digital identity that has been verified. In this manner, the identity proofing and identity provisioning processes are closely connected to the integrity of authenticator, verifying a digital transaction that is initiated by the intended user. As each IAM area impacts the overall security of the transaction, it is important to properly protect each area of the identity lifecycle, according to the acceptable risk level of the service accessed. Projects that are required to use the Veteran-Focused Integration Process (VIP)[3] are subject to

[3] Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) EDP Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National

the VA Assessment and Authorization (A&A) Process,[4] which is based on the Risk Management Framework (RMF).[5] The associated risk assessment will result in a projected authentication assurance level (AAL), which will drive authentication requirements.[6] This document will discuss authenticator and MFA requirements that are related to AAL.

3.1 Overview of Authenticators by Assurance Level

The table below summarizes the requirements for authenticators to meet each of the AALs, as defined by NIST 800-63B. The following abbreviations are used in the table: Single Factor (SF), Multifactor (MF), and One Time Password (OTP). For reference, a personal identity verification (PIV) card is considered a SF Crypto Device and qualifies for AAL 3.

Institute of Standards and Technology (NIST) Publication 800-63A at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[3] Refer to the *VIP 3.2 Guide*, December 2018, at https://vaww.vaco.portal.va.gov/sites/OIT/epmo/vip/Policy%20%20Guidance/VIP%20Guide%203.2.pdf.

[4] Refer to the *VIP Security Guide* at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27; it provides details about the A&A process and how it reflects an implementation of NIST guidance and VA security policies. For additional information on VA A&A, refer to https://www.va.gov/PROPATH/map_library/process_AAA_ext.pdf.

[5] Refer to the NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* at https://pages.nist.gov/800-63-3/sp800-63-3.html. In addition, refer to the VA Handbook 6500, *Risk Management Framework for VA Information Systems*, at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

[6] Refer to the *IAM Risk Assessment* EDP at https://www.oit.va.gov/library/recurring/edp/.

Table 2: Authenticator Requirements by Assurance Level

Requirement	AAL1	AAL2	AAL3

Permitted authenticator types	Look-up Secret;
	Out-of-Band;
	SF OTP Device;
	MF OTP Device;
	SF Crypto Software;
	SF Crypto Device;
	MF Crypto Software;
	MF Crypto Device
		MF OTP Device;
		MF Crypto Software;
		MF Crypto Device;
		Memorized Secret AND:
		• Look-up Secret
		• Out-of-Band
		• SF OTP Device
		• SF Crypto Software
		• SF Crypto Device
			MF Crypto Device;
			SF Crypto Device AND Memorized Secret;
			SF OTP Device AND MF Crypto Device or Software;
			SF OTP Device AND SF Crypto Software AND Memorized Secret

FIPS 140 validation	Level 1	Level 1	MF authenticators - Level 2 Verifiers and SF Crypto Devices - Level 1 Physical security - Level 3
Reauthentication	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity; must use both authentication factors
Security Controls	SP 800-53 Low Baseline	SP 800-53 Moderate Baseline	SP 800-53 High Baseline
Man in the Middle Attack (MitM) resistance	Required	Required	Required
Verifier-impersonation resistance	Not required	Not required	Required
Verifier-compromise resistance	Not required	Not required	Required
Replay resistance	Not required	Required	Required
Authentication intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

3.2 Authenticators Threats

When selecting authenticators and a strategy for MFA, it is important to consider the current threat landscape. There are three common authenticator factors considered when selecting authenticator options: “something you know, something you have, and something you are.” One multifactor authentication method requires the use of two of the three following factors:[7]

- **Something you know** may be disclosed to an attacker. Phishing and keylogging are two common methods of stealing memorized secrets.
- **Something you have** may be lost, damaged, stolen from the owner, or cloned by an attacker. SIM swapping, where an attacker transfers a number to a SIM card in a phone they control, and SMS interception attacks are increasingly used to compromise codes sent to mobile devices.
- **Something you are** may be replicated. Although biometric duplication is not currently common, many devices do not have compatible means to perform biometric authentication.

Additional types of threats include physical attacks, credential service provider (CSP) compromise, and side channels. The probability of exploitation and impact are used to estimate risk when forming mitigation strategies for authenticator use.

3.3 Standard VA User Authenticators

All VA internal users undergo identity proofing before initiating any type of support for VA. The identity proofing process is part of the overall process for the binding and issuance of a PIV card. [8] The PIV card must be used as the standard authenticator for VA staff and must comply with authenticator standards up to AAL 3. It should be noted that the memorized secret personal identification number (PIN) must be six characters in length, if randomly chosen by the CSP or verifier; if chosen by the subscriber, the PIN must be eight characters in length.

3.4 Mobile VA User Authenticators

PIV cards are not used for mobile devices due to a lack of support for PIV card readers. To address this problem, NIST 800-157 was published; it provides guidance for using an alternative authenticator for which issuance is based on the PIV card and its binding to a subscriber, through the identity proofing process. The mobile PIV credential is known as a Derived PIV Credential (DPC), which is a Public Key Infrastructure (PKI) Certificate. There are practices which must be applied to maintain the proper level of risk; this avoids repeating the identity proofing process that is used to issue the PIV card, when provisioning a DPC.

[7] Source: https://www.dhs.gov/sites/default/files/publications/898_ICAM_Common-Appendices_180607-r1.pdf.
[8] Refer to the *IAM Identity Proofing* EDP at https://www.oit.va.gov/library/recurring/edp/.

Hardware-based Authenticators

Hardware authenticators may be physically connected to mobile devices to authenticate, and may qualify for AAL3, if meeting all requirements in Table 2.

- Binding/Provisioning – The user must apply in person, authenticate with their PIV card, and use a biometric.
- Authenticator Compliance – The VA Access and Identity Management (AIM) Program Management Office (PMO) will ensure that the hardware device and CSP meet all compliance criteria for AAL3 in NIST 800-63B and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.[9]

Currently, no hardware DPC tokens are being issued.

Software-based Authenticators

Software-based authenticators must not be rated higher than AAL2. Any SF Crypto Software must be combined with a memorized secret.

- Binding/Provisioning – The user may apply remotely and must authenticate with their PIV card. The application must be initiated from a VA device that is connected to the VA network.
- Authenticator Compliance – VA AIM PMO must ensure that the hardware device and CSP meet all compliance criteria for AAL3 in NIST 800-63B and in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.[10]

3.5 External User Authenticators

External users present several challenges. VA strives to make services accessible to users while balancing the security needed to prevent unauthorized access that could lead to identity theft or fraud. MFA can increase security, but external users may not have a PIV or Common Access Card (CAC); and increasingly, they use mobile devices for access. The maximum expected assurance level for external users is AAL2. Accordingly, authenticator standards are described to meet this requirement.

3.5.1External User Authenticators at AAL1

[9] Ibid. Also refer to the Federal PKI Common Policy Framework at https://pki.treas.gov/docs/x509_certificate_policy_for_the_us_federal_pki_common_policy_framework.pdf.

[10] Ibid.

AAL1 provides minimal assurance that the subscriber controls the determination of the authenticator. As such, any of the authenticators listed in Table 2 are permitted, including a memorized secret as a SF.

3.5.2 External User Authenticators at AAL2 or Higher

For users that require access at AAL2 or higher, hardware-based or software-based authenticators may be used that meet the standards described below. Use of AAL3 for external users is not expected at this time.

Hardware-based Authenticators

Due to the additional cost and administrative overhead of distributing hardware tokens, they are not the primary recommended method of MFA for external users. Hardware tokens may be accepted by the external CSP if a subscriber provides their own hardware token; or if the CSP provides one, it must meet the following requirements:

- Authenticators
    - MF OTP Device
    - MF Crypto Device
    - SF OTP Device and memorized secret
    - SF Crypto Device and memorized secret
- Binding/Provisioning
    - The binding of the authenticator must be performed as part of the identity proofing process.
    - The external CSP must either (a) register the hardware token in connection with a specific device, or (b) require a memorized secret be used with the hardware token.
- Authenticator Compliance – VA AIM PMO must ensure that any external CSP can meet all compliance criteria for AAL2 in NIST 800-63B and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,[11] as part of the CSP approval process.

Software-based Authenticators

Software-based authenticators may be considered at AAL2.

- Authenticators
    - MF Crypto Software
    - SF Crypto software and memorized secret
    - Memorized Secret and Look-up Secret. This method must be restricted to subscribers that do not have a mobile device that supports crypto software. As

[11] Ibid.

both of these factors use static information, it greatly increases the risk that both factors could be captured by phishing, possibly at the same time.
    - Memorized Secret and Out-of-Band (OOB) Device.[12] The following standards may not be used to deliver a secret to an OOB device: VOIP, email, and other methods that do not prove possession of a device; SMS as a communication method with known weaknesses.[13]
- Binding/Provisioning
    - The binding of the authenticator must be performed as part of the identity proofing process.
    - The external CSP must register the software token in connection with a specific device. The software token may not be copied to multiple devices. Each device must be registered separately. Look-up secrets must be mailed to the registered postal address of the subscriber.
- Authenticator Compliance – VA AIM PMO must ensure that any external CSP can meet all compliance criteria for AAL2 in NIST 800-63B and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,[14] as part of the CSP approval process.

4 Application of Practices

The following use case represents application of the MFA practices described in this document.

4.1 Selection of MFA for an External Users

4.1.1 Purpose

Updated Federal policy has been released with new requirements for authentication. External users must comply with new VA policies for authentication to services that access sensitive information. An external CSP is required that is compliant with Federal and VA policy that can provision authenticators to subscribers at AAL2.

4.1.2 Assumptions

- A business justification exists for an external CSP for federation.
- A risk assessment has been completed to determine that AAL2 is required for access to some VA services.
- Once a CSP is determined to be technically viable and approved, a review of the procurement process is outside the scope of this use case.

[12] For more information on account recovery, refer to the *IAM Account Restoration* EDP at https://www.oit.va.gov/library/recurring/edp/.

[13] Sources: https://www.govinfosecurity.com/heres-account-authentication-shouldnt-use-sms-a-11708 and https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/.

[14] Ibid.

4.1.3 Use Case Description

- The system owner has submitted the business case for a solution as a VIP Request (VIPR). The system requires integration with VA IAM for external user access.
- The system owner contacts the VA IAM service to identify available services. As part of the analysis, VA IAM determines that federation with an external CSP is required.
- VA IAM does not have an approved CSP that is compliant with the updated Federal policy yet, and one is not approved through FICAM. A risk assessment is required to approve a new external CSP.
- VA AIM PMO completes the risk assessment for a candidate CSP using vendor-supplied information, or available ATO documentation. The assessment validates the ability to meet technical requirements, the maximum AAL2, and the specific authenticator methods that will be available to subscribers.
- The CSP requests to use a username and password for AAL1, which is approved.
- The CSP requests to use a username and password that is combined with OTP, sent via SMS for AAL2, which is not approved. The VA AIM PMO reviews the approved authenticators with the CSP. The CSP requests to use a username and password, combined with a registered mobile app that provides a software token for subscribers with mobile devices. For subscribers without mobile devices, the CSP requests to use a username and password, combined with a Look Up Secret mailed to the subscriber.
- The CSP is approved for use, VA IAM registers the CSP, and the federation is established.

4.2 Key Practices

Table 5 highlights key practices identified in this EDP.

Table 3: Key Practices IAM Authenticators and MFA EDP

Category	Area	Description
Identity and Access Management	Authenticators and multifactor authentication(MFA)	VA Users: The personal identity verification (PIV) card must be used as the standard authenticator for VA staff and it must comply with authenticator standards up to authentication assurance level (AAL) 3. It should be noted that the memorized secret personal identification number (PIN) must be six characters in length, if randomly chosen by the credential service provider (CSP) or verifier; but if chosen by the subscriber, the PIN must be eight characters in length.
Identity and Access Management	Authenticators and MFA	VA Mobile Users: Hardware authenticators may be physically connected to mobile devices to authenticate,

Category	Area	Description
		and may qualify for AAL3 if meeting all requirements in NIST 800-63B. • Binding/Provisioning – The user must apply in person, authenticate with a PIV card, and use a biometric. • Authenticator Compliance – The VA Access and Identity Management (AIM) Program Management Office (PMO) will ensure that the hardware device and CSP meet all compliance criteria for AAL3 in NIST 800-63B and the X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework.
Identity and Access Management	Authenticators and MFA	VA Mobile Users: Software-based authenticators must not be rated higher than AAL2. Any Single Factor (SF) Crypto Software must be combined with a memorized secret. • Binding/Provisioning – The user may apply remotely and must authenticate with a PIV card. The application must be initiated from a VA device connected to the VA network. • Authenticator Compliance – VA AIM PMO must ensure that the hardware device and CSP meet all compliance criteria for AAL3 in NIST 800-63B and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.
Identity and Access Management	Authenticators and MFA	External Users: The maximum expected assurance level for external VA users is AAL2.
Identity and Access Management	Authenticators and MFA	External Users: AAL1 provides minimal assurance that the subscriber controls the authenticator being used. As such, any of the authenticators listed in NIST 800-63B are permitted, including a memorized secret as a single factor.

Category	Area	Description
Identity and Access Management	Authenticators and MFA	External Users: Hardware tokens may be accepted by the external CSP. If a subscriber provides their own hardware token. or the CSP provides one, it must meet the following requirements: • Authenticators ○ MF OTP Device ○ MF Crypto Device ○ SF OTP Device and memorized secret ○ SF Crypto Device and memorized secret • Binding/Provisioning ○ The binding of the authenticator must be performed as part of the identity proofing process. ○ The external CSP must either (a) register the hardware token in connection with a specific device, or (b) require a memorized secret be used with the hardware token.
		External Users: Software-based authenticators may be considered at AAL2. • Authenticators ○ MF Crypto Software ○ SF Crypto software and memorized secret ○ Memorized Secret and Look-up Secret: This method must be restricted to subscribers that do not have a mobile device that supports crypto software. As both of these factors use static information, it greatly increases the risk that both factors could be captured by phishing, possibly at the same time.

Category	Area	Description
		○ Memorized Secret and Out-of-Band (OOB) Device[15]: The following standards may not be used to deliver a secret to an OOB device: VOIP, email; and other methods that do not prove possession of a device, such as SMS as a communication method, with known weaknesses. • Binding/Provisioning ○ The binding of the authenticator must be performed as part of the identity proofing process. ○ The external CSP must register the software token in connection with a specific device. The software token may not be copied to multiple devices. Each device must be registered separately. Look-up secrets must be mailed to the registered postal address of the subscriber.
Identity and Access Management	Authenticators and MFA	VA IAM PMO must ensure that any external CSP can meet all compliance criteria for AAL2 in NIST 800-63B and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, as part of the CSP approval process.

5 Impacts

If risk management is not used to define the technical requirements for IAM components of VA solutions, the following risks are increased:

- FISMA non-compliance, contributing to a material weakness or other audit findings by external agencies with oversight
- Inadequate technical protections for sensitive data that may contribute to unauthorized access, data breach, or fraud

[15] For more information on account recover, refer to the *IAM Account Restoration* EDP at https://www.oit.va.gov/library/recurring/edp/.

Appendix A: References

- DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx
- FISMA User Stories: https://vaww.portal2.va.gov/sites/asd/AERB/FISMASecurityCompliance/SitePages/Home.aspx
- TRM: http://trm.oit.va.gov/
- NIST 800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision): http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.